AMENDMENTS TO THE CLAIMS

1. (currently amended) A method for synchronizing a ciphering key change in a wireless communications system, the wireless communications system comprising:

a first station capable of receiving a security mode command to effect a ciphering change, and capable of receiving encrypted layer 2 protocol data units (PDUs), each received PDU being sequentially identified by an n-bit frame number (FN), the first station comprising:

~~a first m-bit hyper frame number (HFN); and~~

a decryption unit capable of decrypting received PDUs according to at least a first ciphering key, ~~the~~ a first m-bit hyper frame number (HFN) which is a function of the FN for each received PDU ~~HFN~~, and the FN of each received PDU; and

a second station capable of transmitting the security mode command, capable of assigning each transmitted PDU with an n-bit FN and capable of transmitting encrypted PDUs, the second station comprising:

~~a second m-bit HFN; and~~

an encryption unit capable of encrypting transmitted PDUs according to at least the first ciphering key, ~~the~~ a second m-bit HFN which is a function of the FN for each transmitted PDU, and an FN associated with each transmitted PDU;

the method comprising:

the second station determining an activation time at which a ciphering key change is to occur;

the second station composing the security mode command, the security mode command comprising a switching FN corresponding to the activation time, and x least-significant bits (LSBs) from the second HFN corresponding to the activation time;

the second station transmitting the security mode command;

the first station receiving the security mode command;

the first station utilizing the switching FN and the x LSBs from the second

HFN contained in the security mode command to obtain an application time; and

the first station using the first ciphering key to decrypt PDUs with FNs sequentially prior to the application time, and using a second ciphering key to decrypt PDUs with FNs sequentially on or after the application time, wherein the second ciphering key is different from the first ciphering key.

2. (original) The method of claim 1 wherein the first station increments the first HFN by a predetermined value on detection of roll-over of an FN of a received PDU.

3. (original) The method of claim 1 wherein the second station increments the second HFN by a predetermined value on detection of roll-over of an FN of a transmitted PDU.

4. (original) The method of claim 1 wherein the first HFN and the second HFN are synchronized.

5. (original) The method of claim 4 wherein the activation time corresponds to a second HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted using the second ciphering key, and the application time corresponds to a synchronized first HFN/FN sequence pair for a corresponding received PDU.

6. (original) The method of claim 5 wherein the switching FN is the FN of the crossover PDU, and the x LSBs are extracted from the second HFN corresponding to the crossover PDU.

7. (original) The method of claim 1 wherein the activation time is equal to the application time.

8. (original) The method of claim 1 wherein x is greater than or equal to 2.

9. (original) The method of claim 1 wherein x is equal to m.

10. (original) The method of claim 1 wherein the first station compares the x LSBs from the second HFN contained in the security mode command to determine a cyclical positioning of the switching FN within the first HFN.

11. (currently amended) A wireless communications system comprising:

a first station capable of receiving encrypted layer 2 protocol data units (PDUs), and capable of receiving a security mode command, the first station comprising:

a receiving buffer for storing received PDUs;[[,]]

a means for ~~the first station~~ associating a sequentially ordered n-bit frame numbers (FN) for each received PDU by the first station; ~~and~~

a means for maintaining an m-bit hyper frame numbers (HFN) as a function of the associated FN for ~~with~~ each received PDU by the first station;

an extraction unit for obtaining an application time from a switching FN and x least significant bits (LSBs) of a second HFN, the switching FN and the x LSBs of the second HFN being contained in the security mode command;

a means for storing a first ciphering key;

a means for storing a second ciphering key, which is different from the first ciphering key; and

a decryption unit for decrypting the received PDUs, the decryption unit using the first ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially before the application time, and using the second ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially on or after the application time.

12. (original) The system of claim 11 further comprising a second station capable of transmitting the security mode command, and capable of transmitting the

encrypted PDUs; wherein PDUs that are sequentially before the application time are encrypted using the first ciphering key, and PDUs sequentially on or after the application time are encrypted using the second ciphering key.

13. (original) The system of claim 12 wherein the HFN of each received PDU is synchronized with a corresponding HFN on the second station for each PDU transmitted by the second station.

14. (original) The system of claim 13 wherein the second station comprises an encryption unit capable of generating an activation time, the activation time corresponding to an HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted by the encryption unit using the second ciphering key, and the application time corresponds to a synchronized HFN/FN sequence pair for a corresponding PDU received by the first station.

15. (original) The system of claim 14 wherein the switching FN is the FN of the crossover PDU, and the second HFN is the HFN of the crossover PDU.

16. (original) The system of claim 14 wherein the activation time is equal to the application time.

17. (original) The system of claim 11 wherein the first station increments the HFN associated with a first PDU by a predetermined value on rollover of the FN associated with the first PDU.

18. (original) The system of claim 11 wherein x is greater than or equal to 2.

19. (original) The system of claim 11 wherein x is equal to m.

20. (cancelled)

21. (cancelled)

22. (cancelled)

23. (cancelled)

24. (cancelled)

25. (currently amended) A method for removing cyclical ambiguity of an n-bit identifying frame number (FN) transmitted in a signaling message from a first station to a second station in a wireless communications system, ~~the identifying FN identifying a layer 2 protocol data unit (PDU) in a stream of PDUs, the first station comprising a first m bit hyper frame number (HFN) that is incremented by a first value upon detection of roll-over of an FN in the stream of PDUs, each PDU in the stream of PDUs having an associated FN value and each FN value having an associated HFN value,~~ the method comprising:

the first station placing ~~the~~ an identifying FN for identifying a layer 2 protocol data unit (PDU) in a stream of transmitted PDUs, into a first field of a message;

the first station placing x least significant bits (LSBs) from ~~the~~ a first m-bit hyper frame number (HFN) value associated with the identifying FN in a second field of the message, the first HFN being incremented by a first value upon detection of roll-over of an FN in the stream of transmitted PDUs; and

the first station transmitting the message to the second station;

~~wherein after reception of the message,~~ the second station receiving the message and ~~uses~~ using the x LSBs of the second field to determine a cyclical position of the identifying FN of the first field;

wherein x<m.

26. (original) The method of claim 25 wherein x is greater than or equal to two.

27. (currently amended) The method of claim 25 wherein the second station has a

second HFN that is synchronized with the HFN of the first station, the second HFN being incremented by the first value upon detection of roll-over of an FN in the stream of received PDUs and the second station uses the x LSBs of the second field to determine the cyclical position of the identifying FN within the second HFN.

28. (new) The method of claim 1 wherein x is equal to 2.

29. (new) The method of claim 1 wherein x is less than m.

30. (new) The method of claim 11 wherein x is equal to 2.

31. (new) The method of claim 11 wherein x is less than m.